



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/415,461 | 10/14/1999 | RYUICHI AOKI | 104526 | 4858 |

25944 7590 03/24/2004

OLIFF & BERRIDGE, PLC
P.O. BOX 19928
ALEXANDRIA, VA 22320

| |
|----------|
| EXAMINER |
|----------|

CALLAHAN, PAUL E

| | |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2137

10

DATE MAILED: 03/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

h

Office Action Summary

Application No.

09/415,461

Applicant(s)

AOKI, RYUICHI

Examiner

Paul E. Callahan

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 December 2003.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3 and 5-29 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3 and 5-29 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 14 October 1999 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. Claims 1-13 were pending in this application at the time of the mailing of the previous Office Action. Claim 4 has been cancelled and new claims 14-29 have been added by the latest amendment filed 12-29-2003. Claims 1-3 and 5-29 have been examined.

Response to Arguments

2. The applicant argues in traverse of the rejections of claims 5-11 under 35 USC 112 2nd paragraph that the Examiner is mistaken in believing that the key depository is located on the server. The Examiner respectfully counters that such is not made clear in the language of the claim nor do any of the figures illustrate a depository that is separate from the client or server. The claims are rejected under 35 USC 2nd indefiniteness because the arrangement of elements in the apparatus is not clearly illustrated in the drawing figures and is not clearly defined by the claim language.

3. The Applicant argues in traverse of the rejections of claims 1-4, 12, and 13 under 35 USC 102b) as being clearly anticipated by Fischer '972. The Applicant argues that the claims may be distinguished from the teachings of Fischer since: "the escrow information record is not created or encrypted during the retrieval phase." Yet such a step is not found in the language of the claims. The applicant argues that the escrow information presented by the applicant of Fischer

Art Unit: 2137

must contain: "credentials such as an affidavit..." yet Fischer teaches a more simple protocol in col. 1 lines 44-67 where such information is not required.

The Applicant argues, "Fischer does not disclose or suggest acquiring recovery information decrypted by a private key of the requestor." Yet such is not taught in the claims. Instead, the escrowed information is encrypted under the servers public key, as is taught by Fischer in col. 1 lines 44-67.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1, 12, 13, and 15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The language of claim 5 is directed towards a client-server model. It is unclear from the language of the claims whether the applicant contemplates the depositories as discrete entities or as resident storage areas or modules on the server that communicates with another recovery module on the server via public key encryption. The remaining claims are dependent on claims 1, 12, 13, and 15 respectively and are thereby rejected on the same basis as those claims.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

Art Unit: 2137

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1—3, 5, 7, 12, 13, 15, 16, 18, and 23-26 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Fischer (US 5,436,972).

As per claims 1, 5, 12, 15, and 16, Fischer teaches an encryption key depositing apparatus (Abstract) comprising: a unit that generates an encryption key for a user (col. 1 lines 20-30); and a unit that starts a process in response to the generation of said encryption key (col. 5 lines 24-30, col. 6 lines 25-45), said process allowing a depository deposited with said generated encryption key to store said key in a subsequently recoverable manner (col. 6 lines 25-45), a server and a plurality of clients (abstract), wherein recovery information useable to recover said encryption key is encrypted by the public key of the depository and retained in the server (col. 1 lines 44-67), wherein said server, in response to said recovery request from the depository sends to said depository said recovery information encrypted by said public key of said depository, and acquires from said depository said recovery information decrypted by a private key of said depository and then encrypted by a public key of said server (col. 1 lines 44-67, fig. 5 items 1050, 1060, fig. 1).

As per claim 2, Fischer does not explicitly teach the encryption key depositing apparatus according to claim 1, wherein said encryption key is a private key of a public key cryptosystem, however Fischer does contemplate the user having a public / private key pair (claim 6), and

Art Unit: 2137

contemplates the escrow of all types of secret data (col. 2 lines 24-36). Therefore it is clear that Fischer does contemplate escrow of a user's private key of a public / private key pair.

As per claim 3, Fischer teaches the encryption key depositing apparatus according to claim 1, further having rules established as a basis for determining said depository, said encryption key being stored in accordance with said rules (col. 3 lines 23-30).

As per claims 7 and 18, Fischer teaches a server that, in response to an encryption key recovery request from said depository encrypts said recovered encryption key using said public key of said depository and sends said encrypted recovered encryption key to said depository (col. 1 lines 44-67, fig. 5 items: 1050, 1060).

As per claims 13 and 23-26, the claims represents a computer program product causing an apparatus to carry out the method of claims 1-3, 5, and 7 and are therefore rejected on the same basis as those claims.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2137

9. Claims 6, 8, 17, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer as applied to claim 1 above, and Official Notice taken as detailed below. Fischer does not teach a server log of recovery requests. However it is a step that is old and well known in the art of key escrow for such a log to be kept. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Fischer. It would have been desirable to do so as an added precaution to thwart unauthorized recovery request. Such is taught as a motive to make the combination by Fischer at col. 2 lines 1-7.

Allowable Subject Matter

10. Claims 9-11, 14, 20-22, 27-29 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, second paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period

Art Unit: 2137


will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (703) 305-1336. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is: (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

3/18/04

Paul Callahan


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100